UNITED STATES DISTRICT COURT

DISTRICT OF MINNESOTA

Valerie Anderson, et al., individually and on behalf of all others similarly situated, Plaintiffs, v. Fortra, LLC, Defendant.	Case No. 23-cv-533 (SRN/DTS) CLASS ACTION

PLAINTIFFS' MEMORANDUM IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

State Cases

Statutes

Rules

INTRODUCTION

Defendant Fortra, LLC ("Fortra" or "Defendant") has one primary job: to secure and protect data belonging to others. Defendant did not do the job it undertook, but instead negligently allowed the data with which it was entrusted to be breached. Defendant's failings left Plaintiffs' private data exposed on the dark web where it was used for fraud and theft.

Defendant's arguments for absolving itself from responsibility are unavailing. Plaintiffs have standing to bring their claims as they have suffered specific, concrete injuries and losses. Plaintiffs have sufficiently pleaded a claim for negligence as they have alleged cognizable duties owed to them by Defendant and have adequately pleaded damages. Plaintiffs have a right to declaratory and injunctive relief to better ensure that this does not happen again. Plaintiffs have also properly alleged violations of California consumer protection statutes. For all these reasons, the Court should deny Defendant's motion to dismiss.

FACTS

"Fortra provides global cybersecurity software and services, including the GoAnywhere Managed File Transfer tool for transferring or sharing files." (Mem. Supp. Def.'s Motion to Dismiss Consol. Class Action CCAC [ECF Doc. 52] (hereinafter "MTD") at 2.) Defendant provides these services to a variety of entities, including financial and medical institutions that obtain private personal information from their customers. (Consolidated Class Action Complaint [ECF Doc. 50] (hereinafter "CCAC") ¶ 5.) Defendant knows the importance of data security, given the increased data breach activity

over the past several years, yet it employed inadequate data security and used vulnerable remote access tools. (*Id.* ¶¶ 50-55.) Plaintiffs and Class Members reasonably expected their personal information to be kept private, and Defendant accepted this responsibility and benefited from providing these services, directly and indirectly, to Plaintiffs and Class Members. (*Id.* ¶ 6.)

When necessary to disclose their personal and sensitive information to companies, Plaintiffs did so in with the trust that those companies would protect the data reasonably and competently. (*See, e.g.*, *id,* ¶¶ 132-33, 144-45, 175.) Defendant portrayed itself as expert in the protection of data, offering "services such as vulnerability management, offensive security, email security & Anti-Phishing, Data Protection, Digital Risk Protection, and Secure File Transfer." (*Id.* ¶ 31.) Because Defendant failed to meet its duty to protect Plaintiffs and Class Members' information, it is now in the hands of cybercriminals and circulating on the dark web. (*Id.* ¶¶ 10, 12, 49, 141, 153, 185, 216.)

On January 29, 2023, Defendant discovered that it had been the subject of a data breach and determined either then or shortly thereafter that a malicious third party had gained access to the data Defendant was supposed to be securing (the "Data Breach"). (*Id.* ¶¶ 38-39.) Reports indicate that the hackers gained access to the data of 130 companies that had entrusted Plaintiffs and Class Members personal information to Defendant. (*Id.* ¶¶ 40-41.) "Fortra's own investigation of the Data Breach confirmed that hackers used vulnerabilities in its GoAnywhere MFT and other aspects of its systems, and that millions of individuals were impacted by the Data Breach." (*Id.* ¶ 47.)

Plaintiffs and Class members received notice of the Data Breach approximately a month after it was discovered. (*Id.* ¶ 56.) It is believed that a Russian cybergang, the CLOP ransomware group, or a related group, hacked Defendant's file-transfer system and stole Plaintiffs' personal data as part of a calculated ransomware attack. (*Id.* ¶¶ 7, 12, 41-42, 49.) The Notice confirmed Fortra's systems were breached that the Data Breach was caused, at least in part to "vulnerability[ies] located in [its] software." (*Id.* ¶ 57). The compromised data included names, addresses, phone numbers, Social Security numbers, dates of birth, gender, employer information, insurance information, medical information, including diagnoses and medication, and loan information. (*Id.* ¶¶ 46, 56, 139, 151, 162, 172, 183, 193, 203, 214, 226, 237.) The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. (*Id.* ¶ 118.) The reason cyberthieves take such data is to monetize it on the black market, making it highly likely that Plaintiffs and Class members will feel the repercussions of the theft in tangible ways. (*Id.* ¶¶ 65, 68, 101, 103-04.)

A. Plaintiff Valerie Anderson

Plaintiff Anderson is a citizen of the State of Illinois. (*Id.* ¶ 20.) She was a customer of Hatch Bank, which entrusted her personal information to Defendant. (*Id.* ¶ 127.) Plaintiff Anderson was informed that her name and Social Security number had been compromised in the Data Breach. (*Id.* ¶ 128.) Plaintiff Anderson has subsequently been the victim of fraudulent charges and has received increased spam calls and emails. (*Id.* ¶ 130.) Plaintiff Anderson has suffered emotional distress and has been forced to spend significant time attempting to mitigate the harms caused her by the Data Breach, including

spending multiple hours to monitor financial accounts for fraudulent exploring, as well as registering for and purchasing credit-monitoring services. (*Id.* ¶¶ 131, 136).

B. Plaintiff Danielle Adams

Plaintiff Adams is a resident of Tennessee who obtained medical services through her husband's employer. (*Id.* ¶ 138.) Plaintiff Adams' private information, including her first and last name, date of birth, sex, employer, subscriber ID, member ID, Group ID, address, email address, coverage start and end dates, and Social Security number, were compromised in the Data Breach. (*Id.* ¶ 139.) She has spent approximately 15 hours attempting to mitigate consequences from the substantial risk of additional harm that her and her family face as a result of the Data Breach, and suffered lost time, lost wages, and other lost money due to the Data Breach. (*Id.* ¶¶ 142-43.) Plaintiff Adams has experienced stress and anxiety due to the loss of privacy and the substantial risk of additional harm resulting from the Data Breach. (*Id.* ¶ 148.)

C. Plaintiff Theresa Brewerton

Plaintiff Brewerton is a citizen and resident of North Carolina. (*Id.* ¶ 22.) Plaintiff Brewerton provided her private information to NationsBenefits Holdings, LLC, an administrative services provider to her health insurer. (*Id.* ¶ 150.) NationsBenefits Holdings, LLC entrusted this data to Defendant and on or about April 27, 2023, Plaintiff Brewerton received notice that her full name (including middle initial), gender, Health Plan Subscriber Identification Number, address, phone number, date of birth, and Medicare Number, was compromised by the Data Breach. (*Id.* ¶¶ 150-51.) Plaintiff Brewerton has been the victim of attempted debit card fraud and has suffered a loss of time and money

due to the Data Breach. (*Id.* ¶¶ 152-53.) She has also experienced anxiety and emotional distress related to the fallout from the Data Breach. (*Id.* ¶ 159.)

D. Plaintiff Joseph Cardenas

Plaintiff Cardenas is a resident and citizen of Washington. (*Id.* ¶ 23.) Plaintiff Cardenas provided his private information, through his employer, to a benefits administrator, which employed Defendant. (*Id.* ¶ 161.) On or about April 7, 2023, Plaintiff Cardenas received a Notice of Data Breach informing him that his full name, address, member ID, date of birth, phone number, employer's name, his employer's group ID number, and his coverage and start dates, was compromised by the Data Breach due to Defendant being unable to safeguard the personal information entrusted to it. (*Id.* ¶ 162.) Plaintiff Cardenas has lost time dealing with the Data Breach and has experienced an increase in phishing text messages that demonstrate he is in imminent danger of identity theft. (*Id.* ¶¶ 162-64.) In addition, he has experienced anxiety and emotional distress related to the fallout from the Data Breach. (*Id.* ¶ 169.)

E. Plaintiff Linda Caudill

Plaintiff Caudill resides in Harris County, Texas. (*Id.* ¶ 24.) She was a customer of Hatch Bank, which entrusted her personal information to Defendant. (*Id.* ¶ 171.) Plaintiff Caudill was informed that her name and Social Security number had been compromised in the Data Breach. (*Id.* ¶ 172.) Plaintiff Caudill has received increased spam calls and expended time and money to attempt to mitigate the imminent threat of identity theft. (*Id.* ¶¶ 174-75.) She has also experienced anxiety and emotional distress related to the fallout from the Data Breach. (*Id.* ¶ 180.)

F. Plaintiff Chassidy Holland

Plaintiff Holland is a citizen and resident of Indiana. (*Id.* ¶ 25.) She was required to transfer private information in order to receive medical services, and her service provider employed Defendant to secure her information. (*Id.* ¶ 182.) In late March 2023, Plaintiff Holland was informed that her full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as her date of birth and Social Security number was compromised by the Data Breach. (*Id.* ¶ 183.) Since the Data Breach, Plaintiff Holland has experienced unauthorized bank and credit card charges, unauthorized orders on her amazon account, fraudulent applications for loans and credit cards, a fraudulent tax return filed for her daughter, and her information has been found on the dark web. (*Id.* ¶ 185.) She has been forced to spend substantial time attempting to mitigate the harm arising from the Data Breach, including time spent monitoring her accounts, and driving to and from her bank to address matters. (*Id.* ¶ 186.) She has also experienced anxiety and emotional distress related to the fallout from the Data Breach. (*Id.* ¶ 191.)

G. Plaintiff Mariana Sanchez Lopez

Plaintiff Lopez is a citizen and resident of California. (*Id.* ¶ 26.) She was a customer of Hatch Bank, which entrusted her personal information to Defendant. (*Id.* ¶ 193.) Plaintiff Lopez was informed that her name, date of birth, phone number, email address, and Social Security number had been compromised in the Data Breach. (*Id.*) Plaintiff Lopez has subsequently experienced emotional distress, anxiety, and spent time and effort

to attempt to mitigate the imminent threat of identity theft due to the Data Breach. (*Id.* ¶ 195, 200.)

H. Plaintiff Jennifer Marino

Plaintiff Marino is a citizen and resident of California. (*Id.* ¶ 27.) Plaintiff Marino provided her private information to NationsBenefits Holdings, LLC, an administrative services provider to her health insurer. (*Id.* ¶ 202.) NationsBenefits Holdings, LLC entrusted this data to Defendant and Plaintiff Marino received notice that her full name (including middle initial), gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number was compromised by the Data Breach. (*Id.* ¶ 203.) Plaintiff Marino has since experienced emotional distress in the form of anxiety, a substantial increase in spam calls and emails, and has expended time and money to attempt to mitigate the imminent threat of identity theft. (*Id.* ¶¶ 205-06, 211.)

I. Plaintiff Melissa Morales

Plaintiff Morales is a citizen and resident of California. (*Id.* ¶ 28.) She was a customer of Hatch Bank, which entrusted her personal information to Defendant. (*Id.* ¶ 213.) Plaintiff Morales was informed that at least her name and Social Security number had been compromised in the Data Breach. (*Id.* ¶ 214.) Plaintiff Morales was subsequently the victim of pharmacy fraud, where someone used her name to obtain medicine, requiring substantial time and effort to resolve. (*Id.* ¶ 217.) She has also experienced anxiety and emotional distress related to the fallout from the Data Breach. (*Id.* ¶ 223.)

J. Plaintiff Tara Hartzel Vancosky

Plaintiff Vancosky is a citizen and resident of Pennsylvania. (*Id.* ¶ 29.) She was required to transfer private information in order to receive medical services and her service provider employed Defendant to secure her information. (*Id.* ¶ 225.) Plaintiff Vancosky was informed that her full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as her date of birth and Social Security number, was compromised by the Data Breach. (*Id.* ¶ 226.) Since the Data Breach, Plaintiff Vancosky has experienced a substantial increase in spam calls and has expended substantial time and effort to mitigate the imminent threat of identity theft. (*Id.* ¶¶ 228-29.) She has also experienced anxiety and emotional distress related to the fallout from the Data Breach. (*Id.* ¶ 234.)

K. Plaintiff Muhammad Zahid

Plaintiff Zahid is a citizen and resident of Florida. (*Id.* ¶ 30.) He was a customer of Hatch Bank, which entrusted his personal information to Defendant. (*Id.* ¶ 236.) Plaintiff Zahid was informed that his name and Social Security number had been compromised in the Data Breach. (*Id.* ¶ 237.) Plaintiff Zahid has since experienced stress and anxiety related to the fallout from the Data Breach, a substantial increase in spam calls, texts, and emails, and has expended time and money to attempt to mitigate the imminent threat of identity theft. (*Id.* ¶¶ 239-40, 245.)

STANDARD OF REVIEW

When evaluating a motion to dismiss under Fed. R. Civ. P. 12(b)(6), the Court assumes the facts in the complaint to be true and construes all reasonable inferences in the light most favorable to the plaintiff. *Hager v. Arkansas Dep't of Health*, 735 F.3d 1009, 1013 (8th Cir. 2013). Further, when considering a motion to dismiss, courts "'presum[e] that general allegations embrace those specific facts that are necessary to support the claim.'" *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992) (quoting *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 889 (1990)).

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 556).

ARGUMENT

I. PLAINTIFFS HAVE ARTICLE III STANDING.

Article III of the United States Constitution restricts federal judicial power to resolving "cases" and "controversies" where a plaintiff demonstrates a "personal stake" sufficient to have standing. *Raines v. Byrd*, 521 U.S. 811, 820 (1997). A plaintiff establishes standing by showing: (1) a concrete injury in fact, (2) that is fairly traceable to the defendant's action, and (3) that is likely to be redressed by the relief sought. *Lujan*,

504 U.S. at 560. Here, Defendant challenges two elements of standing in its motion to dismiss—injury in fact and traceability.

To overcome a motion to dismiss for lack of standing, a plaintiff need only "allege sufficient factual matter, accepted as true, to support a reasonable and plausible inference that she satisfies the elements of Article III standing." *Hawse v. Page*, 7 F.4th 685, 688–89 (8th Cir. 2021). "[T]his pleading burden is 'relatively modest.'" *Johnson v. Griffin*, 69 F.4th 506, 510 (8th Cir. 2023) (quoting *Bennett v. Spear*, 520 U.S. 154, 171 (1997)). Here, Plaintiffs have sufficiently alleged concrete injuries-in-fact traceable to Defendant's negligent mismanagement of its network security, which caused the resulting Data Breach and theft of Plaintiffs' highly sensitive information, including social security numbers and medical information. This stolen information is already being misused.

A. Plaintiffs have Alleged Concrete Injuries in Fact Sufficient for Standing.

An "injury in fact" must be "concrete," meaning "'real, and not abstract.'" *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016). A "concrete" injury is an "injury . . . [that] has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *Id.* at 341. Among those harms are economic losses and "reputational harms, disclosure of private information, and intrusion upon seclusion." *TransUnion LLC v. Ramirez*, 141 S.Ct. 2190, 2204 (2021). Additionally, "exposure to [a] *risk* of future harm" is sufficient to establish a "*separate* concrete harm" for standing purposes. *Id.* at 2210 (emphasis added). Courts have repeatedly recognized this harm in the context of a data breach where data breach victims remain at a prolonged and heightened risk of injury. *See Medoff v. Minka Lighting, LLC*, No. 2:22-CV-08885-SVW, 2023 WL 4291973, at *5

(C.D. Cal. May 8, 2023) (collecting cases and holding that "courts across the country have recognized that harms that result as a consequence of a plaintiff's knowledge of a substantial risk of identity theft, including time and money spent responding to a data breach or emotion[al] distress can satisfy concreteness.").

Plaintiffs have adequately alleged an injury in fact by alleging that: (1) Defendant's Data Breach disclosed their sensitive personal information to cybercriminals and purveyors of the dark web, and the "disclosure of private information" is a traditionally recognized harm sufficient for standing; and (2) Plaintiffs expended time and effort mitigating the risk of the Data Breach and suffered emotional distress due to the threat of harm and the exposure of their data. Both of these are sufficient to establish standing where, as here, the Data Breach created a substantial risk of harm.

1. The unauthorized disclosure of Plaintiffs' sensitive private information is an injury in fact.

Courts, including this one, have almost universally found data breach victims have standing where their highly sensitive information was stolen during a data breach. *In re: Netgain Tech., LLC*, No. 21-CV-1210 (SRN/LIB), 2022 WL 1810606, at *5 (D. Minn. June 2, 2022). Despite that, Defendant seeks to dismiss Plaintiffs' complaint on standing grounds, citing the Supreme Court's decision in *TransUnion*, 141 S. Ct. at 2204. (MTD at 10.) However, *TransUnion* only solidifies Plaintiffs' injury-in-fact allegations and confirms they are sufficient for standing here.

In *TransUnion*, the Supreme Court made clear that "injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts"

satisfy Article III's requirement of a "concrete" injury. 141 S. Ct. at 2204. As an example, the Court expressly noted that the "disclosure of private information" constituted a traditional harm affording Article III standing. *Id.*

The data at issue here involves some of Plaintiffs' most personal and private information, like Social Security numbers and medical records. In similar circumstances, courts, including in this District, have held that such serious disclosures of individuals' sensitive personal information in a data breach constitutes a "concrete" injury-in-fact. *See In re Pawn Am. Consumer Data Breach Litig.*, No. 21-CV-2554 (PJS/JFD), 2022 WL 3159874, at *3 (D. Minn. Aug. 8, 2022) (finding plaintiffs' allegation "that their private information (such as Social Security numbers, driver's-license numbers, and financial-account information) [had] been disclosed to cybercriminals . . . [had] a close relationship to disclosure of private information" and was "sufficient to establish standing" (internal quotation marks omitted)); *Perry v. Bay & Bay Transp. Servs., Inc.*, No. 22-CV-973 (JRT/ECW), 2023 WL 171885, at *5 (D. Minn. Jan. 12, 2023) (concluding plaintiff "sufficiently alleged concrete injuries stemming from the data breach" based on facts showing the plaintiff's "PI ha[d] been disclosed to cybercriminals, such injury having a close relationship to a harm traditionally recognized as providing a basis for lawsuits in American courts" (internal quotation marks omitted)); *Florence v. Ord. Express, Inc.*, No. 22-CV-7210, 2023 WL 3602248, at *5 (N.D. Ill. May 23, 2023); *Leonard v. McMenamins, Inc.*, No. 2:22-CV-00094-BJR, 2022 WL 4017674, at *5 (W.D. Wash. Sept. 2, 2022). Even within the last week, courts have recognized standing in such data breach cases – "Like the Supreme Court in *TransUnion*, we have no trouble concluding that [plaintiff's] alleged

harm is sufficiently concrete to support her claims for damages." *Bohnak v. Marsh & McLennan Cos., Inc.*, No. 22-319, 2023 WL 5437558, at *7 (2d Cir. Aug. 24, 2023) (finding exposure of plaintiff's Social Security number and other PII was "concrete" for purposes of Article III standing).

Plaintiffs here have likewise alleged sufficient facts to establish a "concrete" injury. The private information Defendant disclosed was among the most sensitive information a person holds—social security numbers, dates of birth, and private health information. (CCAC ¶¶ 40, 139, 151, 162, 183, 203, 226); *see also Portier v. NEO Tech. Sols.*, No. 3:17-cv-30111, 2019 WL 7946103, at *7–8 (D. Mass. Dec. 31, 2019) (holding, in evaluating standing, that "[b]ecause Social Security numbers are the gold standard for identity theft, their theft is significant"). Indeed, Plaintiffs took significant precautions to keep this information safe both prior to and after the Data Breach. (*See*, *e.g.*, CCAC ¶¶ 132-33, 144-45, 175.) Because of Defendant's negligence, Plaintiffs' sensitive personal information—the type of information individuals generally do not share with anyone else—is now in the hands of cybercriminals and circulating on the dark web for anyone to view. (CCAC ¶¶ 12, 49, 141, 153, 185, 216.) Just as in *Pawn America*, the stolen data's "value derives from the fact that it is private" and that value has been impaired because it "has been published to a third party because of [Defendant's] alleged negligence[.]" 2022 WL 3159874, at *3. That is sufficient for standing, even under *TransUnion.*

Defendant acknowledges that "some courts post-*TransUnion* have analogized [loss privacy from a ransomware attack] to the common-law tort of public disclosure of private fact." (MTD at 18.) But Defendant puts stock in a few hand-selected post-*TransUnion*

cases that found no "concrete" injury based on the loss of privacy. Defendant's cases are highly distinguishable because they either involved the disclosure of non-sensitive information or there was no evidence the hackers obtained the data because it had never been misused or put on the dark web. *See Kim v. McDonald's USA, LLC*, No. 21-CV-05287, 2022 WL 4482826, at *1 (N.D. Ill. Sept. 27, 2022) (noting the "data breach disclosed plaintiffs' non-sensitive information (their email addresses, phone numbers, and delivery addresses), and none of the Plaintiffs had their identities stolen or became the victim of a phishing scam"); *In re Illuminate Educ. Data Sec. Incident Litig.*, No. SACV221164JVSADSX, 2023 WL 3158954, at *1 (C.D. Cal. Apr. 19, 2023) (explaining that "[i]nformation leaked included student academic, behavior, and demographic information," and not "social security, credit card, or bank information"); *In re PracticeFirst Data Breach Litig.*, No. 1:21-CV-00790-JLS, 2022 WL 354544, at *5 (W.D.N.Y. Feb. 2, 2022), *R. & R. adopted*, No. 1:21-CV-790JLS, 2022 WL 3045319 (W.D.N.Y. Aug. 1, 2022) (holding that since the breach was a ransomware attack and the fee was paid, the hacker did not "intend to use the data, in the future, for identity theft or fraud" and noting that none "of the over 1.2 million people affected by the data breach ha[d] experienced attempted or actual identity theft, or a similar type of fraud or attempted fraud, in over a year following the ransomware attack").

Unlike those cases, Plaintiffs here have alleged actual misuse of their stolen data, including: (1) fraudulent charges on a PayPal account; (2) attempted fraudulent charges on a debit card, bank card, and credit card; (3) fraudulent tax returns; (4) fraudulent purchases from Amazon.com; (5) misuse of a Plaintiff's name and date of birth to fraudulently obtain

medications; and (5) increases in phishing texts and emails and spam calls. (CCAC ¶¶ 130, 153, 164, 185, 205, 217, and 228.) Plaintiffs also alleged they received notices that their information was found on the dark web. (*Id.* at ¶¶ 10, 49, 141, 153, 185, and 216.) Thus, unlike *McDonalds* and *Illuminate*, the data at issue here is highly sensitive; and unlike *Practicefirst*, the purpose of the cyberattack here was not just to extort a ransom, but to obtain data to sell to fraudsters who have already misused the data.

Defendant also cites *C.C. v. Med-Data Inc.*, No. 21-2301-DDC-GEB, 2022 WL 970862 (D. Kan. Mar. 31, 2022). There, however, the court misread *TransUnion* as requiring an *additional* showing of "concrete" harm over and above demonstrating a "disclosure of private information." *Med-Data*, 2022 WL 970862, at *10. *TransUnion* made clear, however, that an injury "closely related" to "disclosure of private information," *itself* constitutes "concrete" harm. *See TransUnion*, 141 S. Ct. at 2204 (observing that "intangible harms can also be concrete" and "[c]hief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts," like "disclosure of private information"). Even if the court's analysis in *Med-Data* were accurate, as explained below, Plaintiffs have alleged harms beyond the disclosure of their private data as well, further undermining Defendant's reliance on that case.[1]

[1] Plaintiffs, in fact, also alleged that the exposure of their sensitive information diminished the value of that information. As the Court in *Pawn America* noted, the value of this information derives from the fact it is private. 2022 WL 3159874, at *1. By disclosing it to cybercriminals, that privacy was lost and the value of this information was diminished. *See In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 460-61 (D. Md. 2020) ("[T]he growing trend across courts that have considered this issue is to recognize the lost property value of [personal] information" caused by a data breach and collecting cases holding the same).

The clear weight of authority, including from this District, establishes that the disclosure of Plaintiffs' sensitive personal information to online criminals, as occurred here, is enough to establish an injury-in-fact for standing purposes. On that basis alone, Plaintiffs have standing to bring their claims.

2. The substantial risk of harm created by the Data Breach also comprises an injury-in-fact.

Plaintiffs have also adequately alleged standing based on the substantial and imminent risk of identity theft and the mitigation costs and emotional distress caused by that risk. "[I]f [an] exposure to [a] risk of future harm itself causes a separate concrete harm—for example, a plaintiff's knowledge that he or she is exposed to a risk of future physical, monetary, or reputational harm could cause its own current emotional or psychological harm—then that separate harm may establish standing for a damages claim." *Pawn Am.*, 2022 WL 3159874, at *2 (internal quotation marks omitted). Thus, where "plaintiffs allege a substantial and imminent risk of identity theft" stemming from a data breach, time and money spent "to mitigate the risk of identity theft" qualify as "concrete injuries. *Id.* at *4. Indeed, "[f]ollowing *TransUnion*, courts across the country have recognized that harms that result as a consequence of a plaintiff's knowledge of a substantial risk of identity theft, including time and money spent responding to a data breach or emotion[al] distress can satisfy concreteness." *Medoff*, 2023 WL 4291973, at *4; *Bohnak*, 2023 WL 5437558, at *7-*8; *see also Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 374 (1st Cir. 2023) (collecting cases). Here, Plaintiffs have alleged a

substantial risk of harm that has caused them additional injuries, including mitigation costs and emotional distress.

a. Plaintiffs have sufficiently alleged a substantial or imminent risk of identity theft.

Moreover, even if Plaintiffs must allege the risk of identity is "substantial" or "certainly impending," they eminently do so here.

Courts considering such standards look to several factors. *See e.g., Clemens v. ExecuPharm, Inc.*, 48 F.4th 146, 153 (3d Cir. 2022). Those factors include: (1) whether the data breach was intentional, (2) whether any of the personal data was misused, and (3) whether the personal data is sensitive such that identity theft or fraud is more likely. *See id.* at 153-54; *see also Webb*, 72 F.4th at 375 (noting the Second and Third Circuits consider the same factors). Here, Plaintiffs' allegations satisfy all three factors.

First, Defendant's Data Breach was unquestionably a targeted and intentional criminal act. The complaint alleges that a criminal Russian cybergang, the CLOP ransomware group, or a related group, hacked Defendant's file-transfer system and stole Plaintiffs' personal data as part of a calculated attack. (CCAC ¶¶ 7, 12, 41-42, 49.) Plaintiffs allege that "the reason criminals steal Private Information is to monetize it" on the "black market." (*Id.* ¶ 101.) This is consistent with the Third Circuit's recent observation that "data compromised in a targeted attack is more likely to be misused." *Webb*, 72 F.4th at 375.

Second, the complaint is replete with factual allegations concerning misuse of Plaintiffs' sensitive data, including: instances of actual identity theft and fraud (CCAC ¶¶

130, 153, 185); evidence that Plaintiffs' data is circulating on the dark web (*id.* ¶¶ 141, 153, 185, 216); and facts showing that multiple Plaintiffs saw significant increases in spam and/or phishing communications following the data breach (*id.* ¶¶ 130, 164, 174, 205, 216, 228, 239). "That at least some information stolen in a data breach has already been misused also makes it likely that other portions of the stolen data will be similarly misused." *Webb*, 72 F.4th at 376.

Third, the stolen data here was among the most sensitive and private information possible, including social security numbers, which are difficult to change, and medical records, which are impossible to alter. (CCAC ¶¶ 46, 56.) This "is about the worst kind of private data that one could lose, at least when it comes to creating a risk of identity theft." *Pawn Am.*, 2022 WL 3159874, at *4; *see also Ortiz v. Perkins & Co.*, No. 22-CV-03506-KAW, 2022 WL 16637993, at *4 (N.D. Cal. Nov. 2, 2022) (explaining the theft of information that includes social security numbers creates a sufficient likelihood of future identity theft). The Complaint also alleges facts indicating that criminals consider social security numbers as the "secret sauce" for identity theft because of the many ways they can use those identifiers to impersonate victims. (CCAC ¶¶ 65,68, 103-04.)

Defendant attempts to downplay the substantial risk of identity theft Plaintiffs face by arguing that the purpose of the cyberattack was to extract a ransom, not to commit identity theft. (MTD at 14.) Not so. While the complaint alleges that the data breach occurred as part of a ransomware attack, nothing indicates Defendant ever paid a ransom or the cybercriminals returned or destroyed the data. In fact, the complaint alleges the exact opposite: that the "data is now in the hands of criminals who both have the ability to

misuse the data for fraud or identity theft, and may also sell it to criminals on the dark web capable of doing the same." (CCAC ¶ 49.)

Additionally, Plaintiffs allege their information has already been misused in a variety of fraudulent schemes as a result of the Data Breach. (*Id.* ¶¶ 130, 153, 164, 185, 205, 217, and 228.) That fact distinguishes this case from those Defendant cites. Indeed, in *PracticeFirst*, the "complaint suggest[ed] that defendants' access to the information was ultimately reinstated, presumably after payment of a fee," and there was no allegation of actual misuse of the data. 2022 WL 354544, at *5.[2] Likewise, in *Podroykin v. Am. Armed Forces Mut. Aid Ass'n*, plaintiffs provided no evidence of misuse of data within a 16-month period after the breach and the impacted information was not available on the dark web. No. 1:21-cv-588, 2022 WL 6755834, at *4 (E.D. Va Oct. 11, 2022). Here, by contrast, several Plaintiffs allege that almost immediately after the Data Breach, they either had their data misused, received notice their information was available on the dark web, or both.

Taken together, the alleged misuse of Plaintiffs' data and the notices that their information is already on the dark web so shortly after the Data Breach establishes a "substantial" or "certainly impending" risk of identity theft. *Cf. In re: Netgain Tech.,* 2022 WL 1810606, at *5 (concluding plaintiffs "adequately alleged a substantial risk of future harm" based on the intentional theft of their sensitive data by cybercriminals).

[2] Fortra's reliance on *Graham v. Universal Health Serv.,* 539 F. Supp. 3d 481 (E.D. Pa 2021), and *Quintero v. Metro Santurce, Inc.,* 2021 WL 5855752 (D.P.R. Dec. 9, 2021), is unhelpful, as those cases were recently superseded by the Third Circuit in *Clemens* and the First Circuit in *Webb*, respectively.

b. Plaintiffs have sufficiently alleged injuries in fact due to the substantial risk posed by the Data Breach.

Following *TransUnion*, courts have recognized both mitigation costs and emotional distress are sufficient injuries-in-fact for standing where, as here, a data breach poses a substantial risk of harm. *See Medoff*, 2023 WL 4291973, at *4-5 (collecting cases and explaining that if a "[p]laintiff satisfies the imminence requirement of injury in fact and has shown that he faced a substantial risk of identity theft or fraud" then that plaintiff can establish "a concrete injury through the lost time he has suffered in responding to a substantial risk of identity theft"); *In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1203 (S.D. Fla. 2022) (concluding that "allegations of emotional distress, coupled with the substantial risk of future harm, are sufficiently concrete to establish standing in a claim for damages"). Here, Plaintiffs have alleged they spent both time and effort mitigating the risk of harm created by the Data Breach and suffered emotional harm stemming from the disclosure of their highly private personal and medical information.

Specifically, Plaintiffs have sufficiently pled lost time and money to mitigate the risk of harm flowing from the Data Breach. Those mitigation efforts included: spending multiple hours to monitor financial accounts for fraudulent transactions (CCAC ¶¶ 131, 175, 186, 195, 206, 229, 240); exploring, registering for, and purchasing credit-monitoring services (*id.* ¶¶ 131, 142, 195, 206); and spending time and money driving to and from the bank to address the fallout (*id.* ¶¶ 143, 153, 175, 186). "Because plaintiffs allege a

substantial and imminent risk of identity theft, these mitigation costs qualify as concrete injuries." *Pawn Am.*, 2022 WL 3159874, at *4.

Additionally, Plaintiffs also alleged emotional distress due to the exposure of their private information and the impending risk of identity theft. (CCAC ¶¶ 136, 148, 159, 169, 180, 191, 200, 211, 223, 234, 245.) "[A]lleged emotional distress directly caused by the theft of [] private information" through a cyberattack is "sufficient to establish standing." *Mednax Servs.*, 603 F. Supp. 3d at 1203 (concluding that "allegations of emotional distress, coupled with the substantial risk of future harm, are sufficiently concrete to establish standing in a claim for damages"); *see also Pawn Am.*, 2022 WL 3159874, at *4. The complaint adequately alleges that Plaintiffs experienced emotional distress, including stress and anxiety, caused by the looming threat of identity theft.

In response, Defendant claims Plaintiffs' mitigation efforts are an attempt to manufacture standing by inflicting an injury on themselves in response to a "hypothetical" future harm. (MTD at 13.) That argument fails because the risk here is not hypothetical. (*See supra* § I.A.2.a.) Defendant's effort to cast this risk of future harm as "hypothetical" misses the mark.[3]

For similar reasons, Defendant's attempt to downplay the emotional distress caused by the Data Breach fails. While the *McDonald's* case Defendant relies upon involved

[3] Defendant's argument that Plaintiffs were not injured because they took steps every prudent person should take anyway (MTD at 13) ignores the hours and effort Plaintiffs spent responding directly to the data breach. These efforts went beyond the routine checking of bank accounts and, moreover, Defendant recommended these measures to protect against fraud and identity theft.

purportedly "non-sensitive information," that is not true where the breach involves Plaintiffs' most private and personal data. As Judge Schiltz recently observed, emotional distress caused by cybercriminals stealing *sensitive* personal—"Social Security numbers, driver's-license numbers, and financial account information"—is "sufficient to establish standing." *Pawn Am.*, 2022 WL 3159874, at *4. This case goes even beyond *Pawn America* because the data also includes highly private medical information. Consequently, Plaintiffs have adequately pled emotional harm sufficient for standing.

B. Plaintiffs Allege Injuries Fairly Traceable to Defendant's Conduct.

"An injury is fairly traceable if the plaintiff shows a causal connection between the injury and the conduct complained of that is not the result of the independent action of some third party not before the court." *In re SuperValu, Inc.*, 870 F.3d 763, 768 (8th Cir. 2017) (internal citations omitted); *see also Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 134 (2014) ("Proximate causation is not a requirement of Article III standing, which requires only that the plaintiff's injury be fairly traceable to the defendant's conduct."). As with the burden to show an "injury-in-fact," the pleading standard for traceability is "relatively modest." *Bennett*, 520 U.S. at 171. The court need only make a "threshold" finding that the injury is "fairly traceable" to the defendant's conduct. *Brown v. Medtronic, Inc.*, 628 F.3d 451, 459 (8th Cir. 2010).

Traceability is satisfied in the context of a data breach where: (1) the defendant failed to secure plaintiff's sensitive personal information; (2) the defendant's network was hacked; (3) the plaintiff's sensitive personal information was stolen by the hackers; and (4) the plaintiff suffered identity theft or related injuries after the breach. *Netgain Tech.*, 2022

WL 1810606, at *6; *see also Perry*, 2023 WL 171885, at *5; *Pawn Am.*, 2022 WL 3159874, at *5. Plaintiffs' allegations meet this "relatively modest" burden here. They allege that Defendant failed to secure their sensitive personal information (CCAC ¶¶ 50, 55); that its network was hacked as part of a sophisticated attack by cybercriminals (*id.* ¶¶ 40-41); that Plaintiffs' sensitive personal information was stolen by the cybercriminals (*id.* ¶¶ 40, 46, 139, 151, 162, 183, 203, 226); and that various harms befell Plaintiffs following the breach (*id.* ¶¶ 247-68). At this "threshold" stage, this is sufficient to allege traceability.

Defendant attempts to wave away the connection between its breach and Plaintiffs' harm by arguing that it is impossible to definitively prove a breach caused any attempted or actual fraud, rather than some other cause. (MTD at 20.) But this granular, hyper-technical approach to traceability is inconsistent with the "threshold inquiry for which general allegations of injury, causation, and redressability suffice." *Pawn Am.*, 2022 WL 3159874, at *5 (cleaned up); *see also Perry*, 2023 WL 171885, at *5 ("Bay & Bay's argument that Perry did not provide his bank information is of no moment for establishing standing"). Where a data breach and fraudulent activity occur within such short proximity, plaintiffs have reasonably alleged the data breach caused their injuries. *See S. Indep. Bank v. Fred's, Inc.*, 2:15-cv-0799, 2019 WL 1179396, at *8 (M.D. Ala. March 3, 2019) ("It is nothing more than common sense to say that when two unique events known to bear a causal relationship—a data breach and subsequent fraudulent transactions—occur in the same limited time frame, there is a higher probability that the former caused the latter."); *Stollenwerk v. Tri-West Care Alliance*, 254 Fed. App'x 664, 667 (9th Cir. 2007) ("[T]he fact that the type of information contained on the stolen hard drives is the same type needed

to open credit accounts at the firms where these incidents took place . . . is a matter of common knowledge from which a jury could reasonably draw inference regarding its probative value in establishing causation").

Plaintiffs' allegations satisfy the traceability requirement for standing.

II. PLAINTIFFS ADEQUATELY ALLEGE A CLAIM FOR NEGLIGENCE.

Despite the clear case law in this District supporting negligence claims in similar data breach cases, Defendant makes a cursory attempt to argue that Plaintiffs' fail to adequately allege damages. (MTD at 26-29.) Additionally, Defendant asserts that, under Illinois and Indiana law, it does not have a duty to protect Plaintiffs' information and, furthermore, that Illinois economic loss doctrine bars Plaintiff Anderson's negligence claim. (*Id.* at 29-30.) Defendant is wrong on all accounts.

A. Plaintiffs have Adequately Alleged Damages Suffered Due to the Data Breach.

Defendant asserts that Plaintiffs' "damage[] allegations are insufficient" because they fail "to allege an actual loss or damages to sustain a negligence claim." (MTD at 27.) In doing so, Defendant fails to recognize the prevailing case law in this District.

At the pleading stage, courts are wary of motions to dismiss based on assertions that a plaintiff has not alleged specific damages. *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1171 (D. Minn. 2014) (holding negligence claims would not be dismissed merely because defendant sought a more detailed explanation of the damages alleged); *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 763 (C.D. Ill. 2020) (finding compensable damages under Minnesota negligence claims were sufficiently pled in a class action data breach).

Moreover, Plaintiffs' alleged damages for lost time and credit monitoring are both cognizable damages under the law in this District. *See In re Netgain*, 2022 WL 1810606, at *14 (finding plaintiffs alleged cognizable damages of "loss of time costs, and out-of-pocket expenses" at the pleading stage). Plaintiffs' efforts to mitigate the effects of the data breach and the expenses associated with such efforts establish damages for a negligence claim. *Perry*, 2023 WL 171885, at *8. The Plaintiffs in this case have "suffered numerous and actual concrete injuries as a direct result of the Data Breach," including financial costs incurred mitigating materialized risks, loss of time and productivity, financial costs incurred due to actual identity theft, loss of time following the warnings of the Notice Letter, deprivation of value, and a continued and ongoing imminent risk of future harm. (CCAC ¶ 14.) Indeed, Plaintiffs here have alleged more than merely time lost or emotional distress as damages.[4]

Specifically, Plaintiff Anderson has alleged she suffered damages, and that she has taken steps to mitigate those damages, related to the data breach, including fraudulent

[4] Defendant relies on *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1232 (D. Nev. 2020) to assert that "lost time mitigating the effects of the data breach, emotional distress, … and continued risk to her personal data … are insufficient to support a negligence action." (MTD at 27.) But lost time and emotional damages that are related to tangible, out-of-pocket expenses can be considered cognizable damages. *Pruchnicki*, 439 F. Supp. 3d at 1233. Unlike the plaintiff in *Pruchnicki*, Plaintiffs have alleged tangible out-of-pocket damages. (CCAC ¶¶ 130, 141, 153, 164, 174, 185, 205, 216, 217, 228, 239.) As such, the authority Defendant relies on is unpersuasive. (*See* MTD at 26-27) (citing *Attias v. CareFirst, Inc.*, 365 F. Supp. 3d 1, 13-15 (D.D.C. 2019) (distinguishing between information that has been exposed and misused and information that has merely been exposed but not misused)); *see also Krottner v. Starbucks Corp.*, No. C09-0216RAJ, 2009 WL 7382290, at *7-*8 (9th Cir. Aug. 14, 2009) (waiting to experience an actual loss from identity theft is not the "optimal" approach)).

charges on her PayPal account. (*Id.* ¶¶ 129-131.) After receiving the data breach notice letter and also receiving notice that her information was located on the dark web, Plaintiff Adams spent approximately 15 hours and incurred additional costs attempting to mitigate the substantial risk of future harm, which includes gas money for trips to the bank, and lost wages due to missing work. (*Id.* ¶¶ 142-143.) Plaintiff Brewerton received further notice that her information was located on the dark web after the data breach and has suffered attempted fraudulent charges on her debit card, requiring her to cancel her debit card and spend significant time dealing with the consequences of the financial fraud. (*Id.* ¶ 153.) Plaintiffs Cardenas, Caudill, Lopez, Marino, Morales, Vancosky and Zahid all allege they took specific steps to protect their private information and mitigate the damages following the data breach. (*Id.* ¶¶ 163, 173, 195, 204, 215, 229, 238.) Plaintiff Holland alleged she experienced multiple instances of fraud through unauthorized charges to her bank and credit card, unauthorized orders on her Amazon account, fraudulent applications for loans and credit cards and a fraudulent tax return filed for her daughter,[5] and that her information has been found on the dark web. (*Id.* ¶¶ 185-86.) Additionally, Plaintiff Morales alleged she had to spend significant time with her pharmacy after someone used her name and date of birth to obtain her prescription medication. (*Id.* ¶ 217.)

Moreover, Fed. R. Civ. P. 8's plausibility standard does not create a heightened standard for pleading damages beyond what is necessary to establish standing. *Dieffenbach*

[5] Allegations of actual tax fraud also support Plaintiff's allegations. *Baldwin v. National Western Life Ins. Co.*, No. 2:21-cv-04066, 2012 WL 4206736, at *4, Fn. 1 (W.D. Mo. Sept. 15, 2021).

v. Barnes & Noble, Inc., 887 F.3d 826, 828 (7th Cir. 2018) ("To say that the plaintiffs have standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are available"). Because Plaintiffs have alleged a substantial risk of future harm and Article III standing (*see supra* § I), they have also sufficiently alleged damages.

Plaintiffs have adequately alleged damages arising from their negligence claims, and as such, the Court should deny Defendant's motion.

B. Defendant Had a Duty to Protect Personal Information Under Illinois and Indiana Law.

Defendant argues courts applying Illinois and Indiana law have determined "there is no common law duty to protect personal information to support a negligence claim." (MTD at 29.) Defendant misapplies the current law.

1. Statutory changes in Illinois have created a duty to protect information.

At one time, there was arguably no affirmative duty under Illinois law to protect another from a criminal attack unless a special relationship existed between the parties. *In re SuperValu, Inc.*, 925 F.3d 955, 963 (8th Cir. 2019) (citing *Iseberg v. Gross*, 879 N.E.2d 278, 284-85 (Ill. App. Ct. 2007)); *see also Cmty. Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 816 (7th Cir. 2018) (holding previously that no common law data security duty existed) (citing *Cooney v. Chicago Public Schools*, 943 NE.2d 23 (Ill. App. Ct. 2010)).

However, the *Cooney* case was decided before the Illinois legislature's amendment of the Personal Information Protection Act ("PIPA") in 2017, which now requires data collectors (*e.g.* Defendant) to "implement and maintain reasonable security measures to protect" records from "unauthorized access, acquisition, destruction, use modification, or

disclosure." 815 Ill. Comp. Stat. § 530/45(a). The amendment to PIPA in 2017 calls into question the previous holdings that no duty exists under Illinois law to safeguard Plaintiffs' personal information. *See In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 590 (N.D. Ill. 2022) (declining to dismiss negligence claims based on the non-existence of a data security duty under Illinois law). The current state of Illinois law now arguably *does* place a duty to safeguard consumers' private information.

2. Indiana law has not yet established a general common law, but has found such a duty under the theory of bailment.

Indiana law has not definitively determined whether there is a common law duty to safeguard private information. *Aspen Am. Ins. Co. v. Blackbaud, Inc.*, No. 3:22-cv-44, 2023 WL 3737050, at *3 (N.D. Ind. May 31, 2023); *see also In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 975 (N.D. Cal. 2016) (recognizing that "no Indiana court has yet ruled on" whether Indiana law provides a private cause of action for a negligence claim).

The Southern District of Indiana recently reviewed the issue of duty in a data breach context and determined a duty does exist under the comparable legal theory of bailment. *See Krupa v. TIC Int'l Corp.*, No. 1:22-cv-01951-JRS-MG, 2023 WL 143140, at *3-*4 (S.D. Ind. Jan. 10, 2023) (determining a duty exists because Indiana has "long recognized bailment," which is the "delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose" (citation omitted)). Defendant, as bailee, "must exercise the degree of care commensurate with the benefit" that is being derived. *Id.* Indeed, "[i]n Indiana, bailment law is not reserved for physical goods," but

instead, also applies to "data as a form of property." *See id.* ("[P]roperty means anything of value. The term includes: … data.") (citing Ind. Code § 35-31.5-2-253(a)). Plaintiffs, including Indiana Plaintiff Holland, "each reasonably expected their private information would remain private and confidential, whether the information was provided indirectly or directly to Defendant." (CCPA ¶¶ 5, 48.) Defendant had a duty to exercise reasonable care in holding and securing Plaintiffs' data. (*Id.* ¶¶ 284-88.) Under Indiana law, Defendant thus owed a duty to Plaintiff Holland to securely maintain her private information and her Indiana common law claim of negligence should proceed.

C. Illinois' Economic Loss Doctrine Does Not Bar Plaintiff Anderson's Negligence Claim.

Defendant further argues that Plaintiff Anderson's negligence claim is barred by Illinois' economic loss doctrine. (MTD at 30.) Defendant is wrong for two reasons. First, Plaintiff Anderson alleges she seeks to recover for more than just purely economic losses, but instead for loss of privacy, "stress and anxiety," and lost time as a result of the data breach. CCAC ¶¶ 134, 136. Second, while Plaintiff Anderson has also alleged economic losses, there is no contractual relationship between Plaintiff Anderson and Defendant that would bar her negligence claim.

Under Illinois law, the economic loss doctrine generally "bars a plaintiff from recovering for purely economic losses" in tort where the losses arise out of a failure to perform a contractual obligation. *Perdue*, 455 F. Supp. 3d at 760. The economic loss doctrine does not bar a negligence claim where, like here, Plaintiff alleges both economic and non-economic losses. *See, e.g., Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039

(N.D. Cal. 2019) (economic loss rule did not bar negligence claim where plaintiff also alleged "loss of time," a non-economic harm); *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-cv-2284-H-KSC, 2020 WL 2214152, *4 (S.D. Cal. May 7, 2020) (finding plaintiffs "alleged they have lost time responding to the Breach as well as suffered from increased anxiety and so do not allege purely economic losses"); *In re Ambry Genetics Data Breach Litig.*, No. SACV200079CJCKESX, 2021 WL 4891610, at *4 (C.D. Cal. Oct. 18, 2021) (same). Here, Plaintiff Anderson alleges a variety of non-economic harms, including time and effort spent mitigating the effects of the breach and monitoring accounts, ongoing and continuing risk of identity fraud, loss of use and value of her private information, and suffering from stress and anxiety due to the loss of privacy and substantial risk of additional harm. (CCAC ¶¶ 131, 134, 135, 136.)

Moreover, the Illinois economic loss doctrine does not prohibit recovery in tort where a duty arises outside of a contract. *Sweet v. BJC Health Syst.*, No. 3:20-CV-00947-NJR, 2021 WL 2661569, at *8 (S.D. Ill. June 29, 2021) (recognizing that there was no business relationship between the plaintiff and defendant that would provide for a contractual relationship which would bar plaintiff's negligence claim); *In re Equifax, Inc., Customer Data Security Breach Litig.*, 371 F. Supp. 3d 1150, 1184 (N.D. Ga. 2019) (analyzing Illinois law, and finding that the economic loss doctrine did not apply because parties to the litigation did not have contractual remedies); *see also In re Marriott Int'l, Inc.*, 440 F. Supp. 3d at 475-476 (recognizing that "the policies that underlie" the Illinois economic loss doctrine, "do not translate well to the circumstances of a data breach case").

Defendant itself is quick to point out that "Fortra has no direct interaction with the consumers suing them." (MTD at 1.) Plaintiff Anderson is a consumer affiliated with Hatch Bank, which obtained Plaintiff Anderson's information in order to provide her lending services. (CCAC ¶ 127.) There have been "no interactions, transactions, or dealings" between Plaintiff Anderson and Defendant that could be considered a contractual relationship. (MTD at 1.)

Finally, the two cases Defendant cites do not support its argument: (1) a case where the plaintiffs only alleged economic losses arising from a direct contractual relationship, *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011); and (2) a data breach case where the plaintiffs had a direct contractual relationship with the defendant hospital as customer/patients and alleged only economic damages, *Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 794-95 (W.D. Wis. 2019). (*See* MTD at 30.). Indeed, Defendant has not cited a single case in which the economic loss rule was applied to the relevant facts here, *i.e.*, where the plaintiffs do not have contractual privity with the defendant and where they have alleged non-economic harms.

Plaintiff Anderson has alleged more than just economic damages, and with no contractual relationship, the Illinois economic doctrine cannot apply. The Court should deny Defendant's motion.

III. PLAINTIFFS ADEQUATELY PLEADED A CLAIM FOR NEGLIGENCE *PER SE*.

Plaintiffs' second cause of action asserts a claim for negligence *per se* pursuant to Defendant's violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45

("FTCA"). (CCAC ¶¶ 294-302.) Negligence *per se* "is a form of ordinary negligence that results from violation of a statute." *Anderson v. State*, 693 N.W.2d 181, 189 (Minn. 2005) (citation omitted). Negligence *per se* "substitutes a statutory standard of care for the ordinary prudent person standard of care, such that a violation of a statute (or an ordinance or regulation adopted under statutory authority) is conclusive evidence of duty and breach." *Id.* at 189–90 (citation omitted). Defendant argues that the claim fails for two reasons: (1) Plaintiffs have not adequately alleged they are members of the class of persons the FTCA is intended to protect, and the injury is of the type against which the statute is intended to protect; and (2) because the FTCA does not provide a private right of action. Defendant is wrong on both fronts.

A. The FTCA Is Intended to Protect Persons like the Plaintiffs.

In Minnesota, the only relevant condition in determining whether a violation of the FTCA supports a negligence per se claim is "if the persons harmed by that violation are within the intended protection of the statute and the harm suffered is of the type the legislation was intended to prevent." *Alderman's Inc. v. Shanks*, 536 N.W.2d 4, 8 (Minn. 1995). Congress enacted Section 5 of the FTCA to protect consumers, among others, from "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 244 (1972) (quoting 15 U.S.C.A. § 45). Plaintiffs here are undisputedly consumers and inadequate cybersecurity practices are among those unfair practices barred by the FTCA. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015) (affirming the FTC's enforcement of Section 5 of the FTCA in data breach cases); *cf. In re TJX*

Companies Retail Sec. Breach Litig., 564 F.3d 489, 496 (1st Cir. 2009), *as amended on reh'g in part* (May 5, 2009) (holding allegations that defendants' lack of security measures was "unfair" under the FTCA could support a state unfair-competition claim). Minnesota courts have similarly concluded that a negligence *per se* claim can survive based on Minnesota law. *See, e.g.*, *Perry*, 2023 WL 171885, at *8 (allowing negligence *per se* claim to proceed under Minnesota law).

Plaintiffs and the class have alleged they are members of the group the FTCA was designed to protect. (CCAC ¶¶ 85-91, 96, 117, 288, 296.) Here, Plaintiffs and the class are consumers whose personal information was in the hands of a company which touted itself as a technologically sophisticated protector of data, and whose cybersecurity practices were directly responsible for maintaining the security of consumers' personal information. (*Id.* ¶¶ 3-6.) These allegations are more than the "conclusory" allegations that the Court deemed insufficient in the *Netgain* litigation. *Cf.* 2022 WL 1810606, at *15.

B. The Lack of a Private Right of Action in the FTCA Does Not Preclude a Negligence Per Se Claim.

In Minnesota, a statutory private right of action is not required to bring a negligence per se claim. *See Engvall v. Soo Line R.R. Co.*, 632 N.W.2d 560, 569 (Minn. 2001) (finding "no merit" to argument that lack of a private right of action under the Locomotive Inspection Act precluded railroad worker from alleging his employer's violation to establish duty and breach in a common-law claim for contribution, and plaintiff could have brought a state common law action alleging negligence per se).

In addition, several courts have found a plaintiff may premise negligence *per se* liability on a defendant's violation of Section 5 of the FTCA. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, No. 19-MD-2879, 2020 WL 6290670, at *21-*23 (D. Md. Oct. 27, 2020); *In re Equifax, Inc., Consumer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019); *In re Arby's Rest. Grp. Inc. Litig.,* No. 1:17-CV-0514-AT, 2018 WL 2128441, at *8, *14 (N.D. Ga. Mar. 5, 2018) (noting several courts have held Section 5 of the FTC Act can serve as a basis for a negligence per se claim in the data breach setting); *First Choice Fed. Credit Union v. Wendy's Co.,* No. 16-506, 2017 WL 1190500 (W.D. Pa. Mar. 31, 2017); *Bans Pasta, LLC v. Mirko Franchising, LLC*, No. 7:13-cv-00360-JCT, 2014 WL 637762, at *12–*14 (W.D. Va. Feb. 12, 2014). Courts have allowed claims of negligence *per se* despite lack of a private right of action under Section 5 of the FTC Act where plaintiffs alleged the requisite elements: that defendants violated the statute or rule in question; the rule dictated a standard of conduct or care; the plaintiffs fell within the class of persons the statute was intended to protect; the harm complained of was the same harm the statute was intended to guard against; and violation of the statute proximately caused the plaintiff's injury. *Bans Pasta, LLC*, 2014 WL 637762, at *12–*14.

Here, as in *Bans Pasta*, Plaintiffs pleaded the required elements: Defendants violated the statute or rule in question (CCAC ¶ 90); the rule dictated a standard of conduct or care (*Id.* ¶ 295); Plaintiffs fell within the class of persons the statute was intended to protect (*Id.* ¶ 296); the harm complained of was the same harm the statute was intended to guard against (*Id.* ¶ 297); and Defendants' violation of the statute proximately caused Plaintiffs' injury (*Id.* ¶¶ 300-302).

The Court should allow Plaintiffs' claim for negligence *per se* to proceed.

C. Plaintiffs' Adequately Allege Negligence Per Se *Claims Under Minnesota, Illinois, North Carolina, and Indiana Law.*

Defendant does not challenge that under Illinois law, a negligence *per se* claim can be founded upon a violation of the FTCA. However, it contends that in Florida, Tennessee, Texas, North Carolina, and Indiana, there can be no such cause of action where the relevant statute does not provide for a private right of action. Plaintiffs concede this is true in Florida, Tennessee, and Texas.[6] However, this is not the case in North Carolina and Indiana.

Under North Carolina law, "[t]he negligence *per se* doctrine does not depend on the grant of a private right of action by the legislature and, in the absence of specific legislative exemption, violation of a safety statute generally constitutes negligence as a matter of law." *Makas v. Hillhaven, Inc.*, 589 F. Supp. 736, 741 (M.D.N.C. 1984) (citing *Watson Seafood & Poultry Co., Inc. v. George W. Thomas, Inc.*, 220 S.E.2d 536 (N.C. 1975)). Moreover, " North Carolina courts would allow a negligence *per se* claim based upon a violation of a federal statute, which comports with Fourth Circuit precedent." *Doe v. United States*, 381 F. Supp. 3d 573, 606 (M.D.N.C. 2019) (citing *Fla. Auto Auction of Orlando, Inc. v. United States*, 74 F.3d 498, 502 n.2 (4th Cir. 1996)); *cf. Fulmore v. Howell*, 741 S.E.2d 494, 496 (N.C. Ct. App. 2013) (assuming arguendo that the violation of the Code of Federal Regulations is *per se* negligence). Defendant cites *Hetzel v. JPMorgan Chase Bank, N.A.*,

[6] Plaintiffs Adams, Caudill, and Zahid are thereby foreclosed from asserting claims for negligence *per se*.

No. 4:13-CV-236-BO, 2014 WL 7336863, at *7 (E.D.N.C. Dec. 22, 2014) to support its contention that North Carolina law requires that an underlying statute provide a private right of action. But *Hetzel* made that pronouncement with no supporting caselaw and, in fact, contrary to the caselaw set forth above.

Indiana law recognizes a clear distinction between a negligence *per se* claim and a private right of action and makes clear that the former is not reliant upon the latter. *See, e.g., Stachowski v. Est. of Radman*, 95 N.E.3d 542, 545 (Ind. Ct. App. 2018) ("When a plaintiff claims that the violation of a statute or ordinance gives rise to civil liability even in the absence of a common-law duty, the issue should be framed as whether the statute or ordinance confers a 'private right of action'—a concept that is related to but distinct from the doctrine of negligence *per se*."); *see also Vale Park Animal Hosp., LLC v. Project 64, LLC*, 611 F. Supp. 3d 600, 604–05 (N.D. Ind. 2020) (noting the difference in a private right of action claim and refusing to dismiss plaintiff's claim to the extent is state a cause for negligence *per se*).

Accordingly, Plaintiffs' negligence *per se* claim is adequately pleaded under Minnesota, Illinois, North Carolina, and Indiana law, and Defendant's motion to dismiss that claim should be denied with respect to each of those jurisdictions.

Defendant also contends that Washington, California, and Pennsylvania do not recognize negligence *per se* as a standalone cause of action. Indeed, each of those jurisdictions recognizes negligence *per se* as "an evidentiary doctrine, rather than an independent cause of action." *Jones v. Awad*, 39 Cal. App. 5th 1200, 1210 (Cal. Ct. App. 2019); *see also Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1151

(W.D. Wash. 2017) ("In Washington, however, the violation of a statute or the breach of a statutory duty is not considered negligence *per se*, but may be considered by the trier of fact only as evidence of negligence."). Courts in these states have thus permitted plaintiffs to amend their primary negligence claims to include a negligence *per se* theory. *See, e.g.*, *Sipp-Lipscomb v. Einstein Physicians Pennypack Pediatrics*, No. 20-cv-1926, 2020 WL 7353105, at *1 (E.D. Pa. Dec. 9, 2020) (noting negligence per se theory was "successfully pleaded," but could not be separate from general negligence and allowing Plaintiffs leave to amend); *People of California v. Kinder Morgan Energy Partners, L.P.*, 569 F. Supp. 2d 1073, 1087 (S.D. Cal. 2008). To the extent the Court finds it appropriate to dismiss Plaintiffs' negligence *per se* claim under Washington, California, and Pennsylvania law, it should grant Plaintiffs leave to amend their negligence claim to include a negligence *per se* theory under the laws of those states.

IV. PLAINTIFFS HAVE STANDING TO PURSUE DECLARATORY AND INJUNCTIVE RELIEF.

Defendant argues that Plaintiffs do not have standing to seek declaratory and injunctive relief because they have not alleged "a sufficiently imminent and substantial risk of future harm." (MTD at 33.) However, Defendant reads over critical portions of the CCAC and the caselaw it cites.

Plaintiffs have standing to seek an injunction. To "pursue forward-looking, injunctive relief to prevent" future harm, a plaintiff must allege that the "risk of harm is sufficiently imminent and substantial." *TransUnion*, 141 S. Ct. at 2210. Where "the compromised [personal information] included information such as social security

numbers," and some of the personal information had "allegedly already been used to perpetuate fraud," there is "enough to satisfy standing." *Perry*, 2023 WL 171885 at *4 (denying motion to dismiss claim for injunctive relief to require defendant to improve its data security). As outlined above, Plaintiffs face an ongoing substantial risk of identity theft stemming from the data breach. The attack was intentional, it targeted sensitive personal information (including social security numbers), and it has already resulted in alleged instances of misuse. Like the plaintiff in *Perry*, Plaintiffs here allege a sufficiently imminent and substantial risk of future harm and, therefore, have standing to pursue their claims for injunctive and equitable relief.

Defendant analogizes this case to *Hall v. Centerspace, LP* by arguing that Plaintiffs have failed to allege facts to support that another data breach is "certainly impending" or a "substantial risk," such as Defendant "currently being targeted by hackers" or that "something about their operations makes them uniquely vulnerable to incursions." (MTD at 33 (quoting *Hall v. Centerspace, LP*, No. 22-cv-2028 (KMM/DJF), 2023 WL 3435100, at *3 (D. Minn. May 12, 2023)).) This is simply untrue. Plaintiffs thoroughly allege that cyberattacks and data breaches have been growing increasingly common for years, that their effects can be devastating, and that this was common knowledge. (*E.g.*, CCAC ¶¶ 50–54, 99–111.) Plaintiffs allege that in spite of this knowledge, Defendant chose to not implement cybersecurity measures that not only fell short of best practices, but also failed to meet legal and industry minimum standards. (*Id.* ¶¶ 92–96.) Defendant's record of sub-standard cybersecurity measures and generally laissez-faire practices are the "something

about their operations [that] makes them uniquely vulnerable to incursions." *Hall*, 2023 WL 3435100, at *4.

Moreover, "[t]he risk of another data breach is real, immediate, and substantial" because, as Plaintiffs allege, "Defendant's data security measures remain inadequate." (CCAC ¶¶ 306, 309.) Defendant may argue that Plaintiffs have not substantiated this allegation, but at this stage, the Court "must accept the allegations contained in the complaint as true and draw all reasonable inferences in favor of the nonmoving party." *Coons v. Mineta*, 410 F.3d 1036, 1039 (8th Cir. 2005) (citation omitted); *Hall*, 2023 WL 3435100, at *2. These allegations are sufficient at this stage. (*See* CCAC ¶ 305 ("An actual controversy has arisen in the wake of the Data Breach regarding . . . whether Defendant currently maintains data security measures adequate to protect Plaintiffs and Class Members from further data breaches that threaten the Private Information in Defendant's possession.").)

In contrast, the plaintiffs in *Hall* alleged only that they suffered "continued risk to their PII." 2023 WL 3435100, at *2. Notably, they also alleged that the defendant implemented cybersecurity measures after the breach, *id.* at *1; there is no such allegation here (*see generally* CCAC). The *Hall* Court found that "[n]othing in [the complaint] transforms the possibility that Centerspace might suffer another data breach into an imminent or substantial risk." 2023 WL 3435100, at *4. The court made clear that it was "not suggesting that forward-looking injunctive relief is never appropriate in a data breach case," and distinguished that case from one recently decided by this Court on the grounds that the latter had "far more substantial" allegations. *Id.* (citing *Perry*, 2023 WL 171885).

Finally, Defendant's attempts to distinguish *In re Netgain Technology, LLC* are without merit. Defendant contends this Court held that the *Netgain* plaintiffs had standing to seek an injunction because they sought a declaration that the defendant "owed and continues to owe" them a duty, which Defendant argues "was both forward- and backwards-looking." (MTD at 34.) There are three flaws with this argument. First, Plaintiffs here seek a declaration that Defendant "continues to owe a legal duty," and the distinction between "continues to owe" on the one hand, and "owed and continues to owe" on the other, is semantical at best. Second, the plaintiffs in both this case and in *Netgain* brought negligence claims, which require a finding that the defendants owed them a duty, rendering a declaration to that effect superfluous. Third, and most importantly, Defendant contradicts itself. Defendant's argument in all but this final paragraph is that to have standing to bring a claim for "forward-looking" injunctive relief, the plaintiff must allege that an injunction would prevent against an imminent or sufficiently high risk of harm. Defendant fails to explain how including a "backward-facing" declaration affects the standing analysis for the prospective relief; it doesn't.

For these reasons, as it did in *Netgain* and *Perry*, the Court should conclude that Plaintiffs have standing to seek their declaratory and injunctive relief.

V. PLAINTIFFS HAVE ALLEGED VALID CLAIMS FOR INJUNCTIVE RELIEF UNDER THE CALIFORNIA CONSUMER RECORDS ACT.

Defendant contends that the California Customer Records Act ("CRA") *only* creates a private right of action for direct customers of a business. (MTD at 34-35.) Not so. Neither

the statute's text nor relevant caselaw support Defendant's argument that the CRA applies only to direct customers of a breached entity.[7]

The CRA is not limited to protecting California residents who qualify as a business's direct customers. Section 1798.81.5(a)(1) of the CRA states: "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected" and "encourage[s] businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information." Subsection (a)(2) specifically states "the terms 'own' and 'license' include personal information that a business retains as part of the business' internal customer account . . . [and t]he term 'maintain' includes personal information that a business maintains but does not own or license. Cal. Civ. Code § 1798.81.5. If a data breach occurs, the CRA requires the breached entity to provide notice to all affected California residents regardless of whether the victims are the breached business's customers. *See* Cal. Civ. Code § 1798.82(a) and (b). Moreover, the plain language of subsection (e) states: "Any business that violates, proposes to violate, or has violated this title may be enjoined." Cal. Civ. Code § 1798.84(e). As California residents victimized by the Data Breach, Defendant violated § 1798.82 of the CRA by failing to provide timely notice to its customers and non-customers alike. Therefore, California Plaintiffs may bring this action seeking an injunction of Defendant's conduct pursuant to Cal. Civ. Code §§ 1798.82 and 1798.84(e).

[7] California Plaintiffs concede that as non-customers of Defendant, they can only seek injunctive relief under § 1798.84(e) (rather than damages and penalties available to "customers" under §§ 1798.84(b) through (d)).

Supporting this interpretation of the statutory language, the court in *Castillo v. Seagate Tech., LLC*, found that "[a]lthough the CRA is primarily concerned with the protection of customer data, . . . and provides remedies only for customers harmed by its violation, . . . its plain language nonetheless operates to protect some non-customer information." No. 16-CV-01958-RS, 2016 WL 9280242, at *7 (N.D. Cal. Sept. 14, 2016) (citations omitted); *see also Portier*, 2019 WL 7946103, at *23 (citing Cal. Civ. Code §§ 1798.81.5(a)-(b), 1798.82).

The Court should deny Defendant's motion to dismiss the California Plaintiffs' CRA claim.

VI. PLAINTIFFS PROPERLY ALLEGE DEFENDANT'S VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW.

Defendant's contention that Plaintiffs Lopez, Marino, and Morales fail to state a claim for Defendant's violation of California's Unfair Competition Law, Cal. Bus. Code § 17200, *et seq*. ("UCL"), itself fails to account for the entirety of Plaintiffs' allegations, as well as both Eighth Circuit and Ninth Circuit law.

Defendant's claim that Plaintiffs must allege the lack of an adequate remedy at law is contrary to Fed. R. Civ. P. 8(d)(3), which provides, "[a] party may state as many separate claims or defenses as it has, regardless of consistency." Likewise, Rule 8(a)(3) provides that a pleading must include "a demand for the relief sought, which may include relief in the alternative or different types of relief." A plaintiff may "present[] two alternative—as opposed to duplicative—theories of liability and is allowed to plead both. The plaintiff is simply not allowed to recover twice." *Silva v. Metro. Life Ins. Co.*, 762 F.3d 711, 726 (8th

Cir. 2014) (citations to rules omitted); *see also* Fed. R. Civ. P. 18 ("A party asserting a claim ... may join, as independent or alternative claims, as many claims as it has against an opposing party"); *Jackson v. FindJodi.com, Inc.*, No. 21-CV-1777 (SRN/DTS), 2022 WL 336832, at *3 (D. Minn. Feb. 4, 2022), *aff'd sub nom. Jackson v. Find Jodi.com, Inc.*, No. 22-1652, 2022 WL 4455209 (8th Cir. June 1, 2022) (citing Fed. R. Civ. P. 18); *Garman v. Griffin*, 666 F.2d 1156, 1159 (8th Cir. 1981); *City of Columbia, Missouri v. Elliott Equip. Co.*, No. 2:19-CV-04042-BCW, 2019 WL 13156313, at *3 (W.D. Mo. July 17, 2019). The fact that Plaintiffs do not explicitly acknowledge any inconsistency or alternative pleading in the Complaint has no bearing. This Court held under similar circumstances that, "[a]s [plaintiff] is the nonmoving party, the Court will construe its pleadings in the most favorable light and assume that [plaintiff] disputes the existence of an [adequate remedy at law] for the purposes of its equitable claims." *Goodbye Vanilla, LLC v. Aimia Proprietary Loyalty U.S. Inc.*, 304 F. Supp. 3d 815, 824 n. 6 (D. Minn. 2018) (citing Rule 8).[8]

Ninth Circuit precedent is to similar effect. *See, e.g., Olympic Coast Inv., Inc. v. Seipel*, 208 F. App'x 569, 571 (9th Cir. 2006) (plaintiffs' assertion of inconsistent and alternative claims may not be construed as a waiver of their rights to recovery under either claim) (citing *Ryan v. Foster & Marshall, Inc.*, 556 F.2d 460, 463 (9th Cir. 1977)). The sole Ninth Circuit appellate case Defendant cites in this context provides only that "a plaintiff 'must *establish* that she lacks an adequate remedy at law before securing equitable

[8] *See also Ikechi v. Verizon Wireless*, No. 10-CV-4554 JNE/SER, 2011 WL 2118797, at *6 (D. Minn. Apr. 7, 2011), *report and recommendation adopted*, No. Civ. 10-4554 JNE/SER, 2011 WL 2118791 (D. Minn. May 25, 2011) (allowing equitable claim despite lack of reference to alternative pleading, citing Rule 8).

restitution for past harm under the UCL.'" (MTD at 36 (quoting *Sonner v. Premier Nutr. Corp.*, 971 F.3d 834, 844 (9th Cir. 2020) (emphasis added).) But *Sonner* says nothing about pleading standards, as the case addressed a district court proceeding in which the plaintiff dropped all its legal claims on the eve of trial so as to secure a bench trial. 971 F.3d at 937.

For that reason, Ninth Circuit district courts have repeatedly held that *Sonner* has no bearing at the pleading stage. Most recently, the Ninth Circuit held that "*Sonner* has limited applicability to the pleading stage and the general liberal policy courts have toward pleading in the alternative allow[s] [an] equitable restitution claim to proceed past the pleading stage even though the plaintiff [is] also seeking" a remedy at law. *Warren v. Whole Foods Mkt. California, Inc.*, No. 21-CV-04577-EMC, 2022 WL 2644103, at *9 (N.D. Cal. July 8, 2022) (citing *Nacarino v. Chobani, LLC*, No. 20-CV-07437-EMC, 2022 WL 344966, at *10-12 (N.D. Cal. Feb. 4, 2022)); *see also Marshall v. Danone US, Inc.*, 402 F. Supp. 3d 831, 834 (N.D. Cal. 2019) (allowance of equitable claims in addition to legal claims at pleading stage is "more consistent with ordinary pleading principles," distinguishing *Mullins v. Premier Nutrition Corp.*, No. 13-cv-01271-RS, 2018 WL 510139 (N.D. Cal. Jan. 23, 2018) (*cited in* MTD at 37)[9]; *see also Linton v. Axcess Fin. Servs., Inc.*, No. 23-CV-01832-CRB, 2023 WL 4297568, at *3 (N.D. Cal. June 30, 2023). Defendant's

[9] *See also Jeong v. Nexo Financial LLC*, No. 21-cv-02392-BLF, 2022 WL 174236, at *27 (N.D. Cal. Jan. 19, 2022) (distinguishing *Sonner* based on its procedural posture, citing additional cases); *Rothman v. Equinox Holdings, Inc.*, No. 2:20-cv-09760-CAS-MRWx, 2021 WL 1627490, at *12 (C.D. Cal. Apr. 27, 2021) (same).

contention that Plaintiffs Lopez, Marino, and Morales's UCL claim is improper is, at best, premature at this pleading stage of the case.

Defendant's additional contention that Plaintiffs Lopez, Marino, and Morale lack standing for not having alleged any loss of money or property rests on even weaker ground. As Plaintiffs allege:

> Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service or product that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer network and Plaintiffs and Class Members' Private Information.

(CCAC ¶ 264); *see also Tellabs, Inc. v. Makor Issues & Rights., Ltd.*, 551 U.S. 308, 322 (2007) ("[C]ourts must consider the complaint in its entirety… when ruling on Rule 12(b)(6) motions to dismiss …").

Moreover, Defendant cites only one case in this context – *Kwikset Corp. v. Superior Ct.*, 246 P.3d 877 (Cal. 2011). (MTD at 37.) The *Kwikset* court observed that "[t]here are innumerable ways in which economic injury from unfair competition may be shown. A plaintiff may … (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." 246 P.3d at 885-86. Plaintiff Morales alleges exactly that. (*See* CCAC ¶ 217 ("Plaintiff Morales was also required to make multiple in person visits to her pharmacy, causing her to consume gasoline that she paid for.").) Finally, "[c]ourts in California have consistently held that benefit of the bargain damages represents economic injury for purposes of the UCL. … Taken together, *Kwikset* [and other cases] demonstrate that benefit of the bargain losses, as alleged in the consolidated

amended complaint, constitute economic injury cognizable under the UCL." *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp. 3d 1284, 1301 (S.D. Cal. 2020) (citations omitted).

Defendant's assertion that "plaintiffs are not entitled to restitution because they do not … plausibly allege that Defendant received any funds from plaintiffs, either directly or indirectly" (MTD at 37) is also contrary to the Complaint. (*See* CCAC ¶ 264 ("Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer network.").) And despite acknowledging that its indirect receipt of funds from Plaintiffs would entitle them to restitution, Defendant quotes *Korea Supply Co. v. Lockheed Martin Corp.*, 63 P.3d 937, 947 (Cal. 2003), for the premise that "[a]ny award that plaintiff would recover from defendants would not be restitutionary as it would not replace any money or property that defendants took *directly* from plaintiff." (MTD at 37 (emphasis added).) In any event, the California Supreme Court held well after *Korea Supply Co.* that UCL plaintiffs may seek restitution for their indirect payments to defendants. *See, e.g., Clayworth v. Pfizer, Inc.*, 233 P.3d 1066, 1087 (Cal. 2010). Finally, *Fresno Motors, LLC v. Mercedes Benz USA, LLC*, is inapposite, as it addressed "a loss by the plaintiff without any corresponding gain by the defendant." 771 F.3d 1119, 1135 (9th Cir. 2014). That is not this case.

Defendant cites *Sun Microsystems, Inc. v. Microsoft Corp.*, 188 F.3d 1115, 1123 (9th Cir. 1999), for the proposition that a UCL "plaintiff cannot receive an injunction for past conduct unless he *shows* that the conduct will probably recur." (MTD at 38 (emphasis added).) But like *Sonner*, *Sun Microsystems* says nothing about the pleading stage. In this

case, Plaintiffs allege that: Defendant misrepresented the security of its systems prior to the Data Breach (CCAC ¶¶ 31, 49); "[t]he risk of another data breach is real, immediate, and substantial" (*id.* ¶ 309); that "Plaintiff Morales was notified by a third-party monitoring service that her Social Security number was located on the dark web" (*id.* ¶ 216); and Plaintiffs' "Private Information … remains in the possession of Defendant, and … is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it." (*Id.* ¶ 14.)

The court in *In re Yahoo! Inc. Customer Data Sec. Breach Litig.* held that similar allegations were sufficient to state a claim for injunctive relief pursuant to the UCL:

> [A] fair reading of the [complaint] is that, although Defendants "claim[ ] to have plugged the leaks" in their security systems, Plaintiffs cannot trust Defendants' representations regarding their security systems. Accordingly, Plaintiffs face a "real and immediate threat" of further disclosure of their PII, which remains in the hands of Defendants. … Moreover, Plaintiffs allege that … hackers have been actively selling the PII of Defendants' users on the dark web. … Plaintiffs allege that Defendants have not only failed to take any actions with regard to this information being on the dark web, but that Defendants have continued to dispute the scope of their responsibility. … Taking these allegations as true and in the light most favorable to Plaintiffs, the Court finds that Plaintiffs have adequately alleged a "real and immediate threat of repeated injury" from Defendants.

No. 16-MD-02752-LHK, 2017 WL 3727318, at *11 (N.D. Cal. Aug. 30, 2017); *see also Mehta v. Robinhood Fin. LLC* , No. 21-CV-01013-SVK, 2021 WL 6882377, at *11 (N.D. Cal. May 6, 2021).

For all these reasons, Plaintiffs' allegations in this case are more than sufficient o state a claim for injunctive relief under the UCL.

VII. PLAINTIFFS ALLEGE VALID CLAIMS UNDER THE CALIFORNIA CONSUMER PRIVACY ACT.

The California Consumer Privacy Act ("CCPA") provides a private right of action against a "business" that fails to implement and maintain reasonable data security measures. Cal. Civ. Code § 1798.150(a)(1). A "business" is defined in relevant part as a company "that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information …." Cal. Civ. Code Ann. § 1798.140(d)(1). This should "be liberally construed to effectuate [the CCPA's] purposes." Cal. Civ. Code Ann. § 1798.194. Yet, Defendant interprets this provision narrowly, arguing that it is not a "business" because (1) it does not collect consumer information directly from consumers, and (2) it does not control the "purposes and means of the processing of consumers' personal information." (MTD at 48-49.)[10] Instead, Defendant argues that it is a "service provider," which is subject to administrative—not private—action under the CCPA. (*Id.*)[11]

---

[10] Defendant also argues that Plaintiffs' CCPA claim should fail because Plaintiffs allege Defendant collects the personal information of "its employees"—rather than consumers. (MTD at 49 (citing CCAC ¶ 343).) Defendant appears to acknowledge that this was a scrivener's error—Plaintiffs Morales, Lopez, and Marino are consumers, not Defendant's employees. (*See* CCAC ¶¶ 193, 202, 213.) Regardless, even an employee constitutes a "consumer" under the CCPA since a "consumer" is simply defined as "a natural person who is a California resident …." Cal. Civ. Code Ann. § 1798.140(i).

[11] A "service provider" is defined as "a person that processes personal information on behalf of a business and that receives from or on behalf of the business consumer's personal information for a business purpose pursuant to a written contract …." Cal. Civ. Code Ann. § 1798.140(ag)(1).

Defendant need not collect information directly from consumers to be a "business" under the statute. This overlooks the definition of the word "collects," which encompasses consumer data obtained "*by any means*." *See* Cal. Civ. Code Ann. § 1798.140(f) (emphasis added).[12] Here, Plaintiffs allege that "in the ordinary course of Fortra's business, Defendant gains access to, acquires, possesses, analyzes, and otherwise utilizes personally identifiable information, including, but not limited to Plaintiffs' and putative Class Members' names and Social Security numbers." (CCAC ¶ 4.)

Plaintiffs also adequately allege that Defendant (alone or jointly with others) controlled the means of "processing" Plaintiffs' personal information after it was obtained.[13] *Compare, e.g., In re Blackbaud, Inc., Customer Data Breach Litig.*, No. 3:20-MN-02972-JMC, 2021 WL 3568394, at *5 (D.S.C. Aug. 12, 2021) (declining to dismiss CCPA claim against company that "develops software solutions to process its customers' patrons' personal information.") *with* (CCAC ¶ 33 (Defendant was hired "to manage access to and store and protect Plaintiffs' … Private Information.") *and id.* ¶ 34 (Defendant "accept[ed] and gain[ed] control over Plaintiffs' and Class Members' Private Information ….")).

---

[12] In full, the CCPA states that "collects" or "collected" under the CCPA "means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior." Cal. Civ. Code Ann. § 1798.140(f).

[13] Under the CCPA, "processing" means "any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means." Cal. Civ. Code Ann. § 1798.140(y).

For the foregoing reasons, Defendant is a "business" under the CCPA. To the extent Defendant is also a "service provider," this is irrelevant. *See Blackbaud*, 2021 WL 3568394, at *5-6 ("[T]he statutory definition of 'service provider' suggests that 'business' is a broader term …. Because Blackbaud could be both a 'service provider' and a 'business' under the CCPA, it would not be insulated from liability under the CCPA if it qualified as a 'service provider.' Consequently, the court need not consider whether Blackbaud is a 'service provider' under the CCPA ….").

For all these reasons, the Court should allow Plaintiffs' claim under the CCPA to proceed.

CONCLUSION

Defendant's motion to dismiss fails to appreciate the legal landscape of decisions in this District concerning data breaches. The facts and the law demonstrate that Plaintiffs have concrete traceable injuries to constitute standing for their claims. Defendant's swings at Plaintiffs' specific causes of action are unavailing. Plaintiffs have more than adequately pled negligence, negligence per se, declaratory judgment, and violation of three of California's consumer protection statutes. Defendant's assertions to the contrary fail to account for the current procedural posture, find no support in the law, and are countered by Plaintiffs' factual allegations.

The Court should deny Defendant's Motion to Dismiss in its entirety.

Respectfully submitted,

Dated: August 28, 2023

s/ Bryan L. Bleichner

Bryan L. Bleichner (MN #0326689)
Christopher P. Renz (MN #0313415)
Philip J. Krzeski (MN #0403291)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
bbleichner@chestnutcambronne.com
crenz@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Brian C. Gudmundson (MN #336695)
Michael J. Laird (MN #398436)
Rachel K. Tack (MN #399529)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Phone: (612) 341-0400
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Interim Co-Lead Class Counsel

Nathan D. Prosser (MN #0329745)
Anne T. Regan (MN #0333852)
HELLMUTH & JOHNSON PLLC
8050 West 78th Street
Edina, MN 55439
Phone: (952) 746-2124
nprosser@hjlawfirm.com
aregan@hjlawfirm.com

Joseph M. Lyon*
THE LYON LAW FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
jlyon@thelyonfirm.com

Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Phone: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
tcoates@msdlegal.com
dgould@msdlegal.com

Daniel E. Gustafson (MN #0202241)
David A. Goodwin (MN #0386715)
Joe E. Nelson (MN #0402378)
GUSTAFSON GLUEK PLLC
120 South Sixth Street, Suite 2600
Minneapolis, MN 55402
Phone: (612) 333-8844
dgustafson@gustafsongluek.com
dgoodwin@gustafsongluek.com
Jnelson@gustafsongluek.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

John G. Emerson*
EMERSON FIRM, PLLC
2500 Wilcrest Drive, Suite 300
Houston, TX 77042-2754
Phone: (800) 51-8649
jemerson@emersonfirm.com

Bart D. Cohen*
BAILEY & GLASSER LLP
1622 Locust St.
Philadelphia, PA 19103
Phone: (267) 973-4855
bcohen@baileyglasser.com

Karen Hanson Riebel (MN #0219770)
Kate M. Baxter-Kauf (MN #0392037)
LOCKRIDGE GRINDAL NAUEN, P.L.L.P.
100 Washington Ave. South, Ste. 2200
Minneapolis, MN 55401
Phone: (612) 339-6900
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

John A. Yanchunis*
Marcio W. Valladares*
Ra. O. Amen*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin St. 7th Floor
Tampa, Florida 33602
Phone: (813) 223-5505
jyanchunis@forthepeople.com
mvalladares@forthepeople.com
ramen@forthepeople.com

Kenneth J. Grunfeld*
Kevin W. Fay*
GOLOMB SPIRT GRUNFELD P.C.
1835 Market St., Ste. 2900
Philadelphia, PA 19103
Phone: (215) 346-7338
Facsimile: (215) 985-4169
kgrunfeld@golomblegal.com
kfay@golomblegal.com

Executive Committee Counsel for Plaintiffs and the Putative Class

**Admitted pro hac vice*